DOI:
10.1112/blms.12199

Document Version
Peer reviewed version

ON THE BIRCH–SWINNERTON-DYER CONJECTURE AND SCHUR INDICES

MATTHEW BISATT AND VLADIMIR DOKCHITSER

Abstract. For every odd prime p, we exhibit families of irreducible Artin representations τ with the property that for every elliptic curve E the order of the zero of the twisted L-function $L(E,\tau,s)$ at $s=1$ must be a multiple of p. Analogously, the multiplicity of τ in the Selmer group of E must also be divisible by p. We give further examples where τ can moreover be twisted by any character that factors through the p-cyclotomic extension, and examples where the L-functions are those of twists of certain Hilbert modular forms by Dirichlet charaters. These results are conjectural, and rely on a standard generalisation of the Birch–Swinnerton-Dyer conjecture. Our main tool is the theory of Schur indices from representation theory.

1. Making the analytic rank divisible by p

There is a standard "minimalist conjecture" that generically the L-function of an elliptic curve vanishes to order 0 or 1 at $s=1$, depending on the sign in the functional equation. As we will illustrate, this has to be used with some caution: even when the associated Galois representation is irreducible, certain L-functions cannot vanish to order 1 at $s=1$ — the order of their zero should be a multiple of a (possibly large) integer n.

More precisely, we look at twists of elliptic curves E by Artin representations τ and their L-functions $L(E,\tau,s)$, that is the L-function associated to the tensor product of τ with the Galois representation of E. When τ factors through $F/\mathbb{Q}$ this is a factor of $L(E/F,s)$, much like the Artin L-function $L(\tau,s)$ is a factor of the Dedekind ζ-function of F.

Throughout the article p and q will be distinct odd primes. We write $\langle\ ,\ \rangle$ for the usual inner product of characters of representations of finite groups (embedding them into $\mathbb{C}$ if necessary): thus $\langle X,\tau\rangle$ is the multiplicity of τ in X if τ is irreducible.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve. Let τ be an irreducible faithful Artin representation of a Galois extension $F/\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q})\cong C_q\rtimes C_{p^n}$ non-abelian and with $p^n\nmid q-1$.*
(i) If the Birch–Swinnerton-Dyer conjecture for Artin twists (Conjecture 2.1) holds, then

$$\mathrm{ord}_{s=1}\,L(E,\tau,s)\equiv 0 \mod p.$$

(ii) If the ℓ-primary part of the Tate–Shafarevich group $Ш(E/F)[\ell^\infty]$ is finite, then

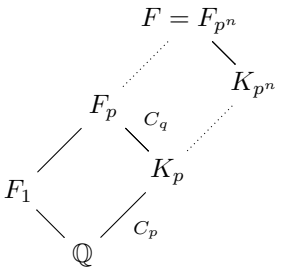
$$\langle X_\ell(E/F),\tau\rangle\equiv 0 \mod p,$$

where ℓ is any prime and $X_\ell(E/F)$ is the Pontryagin dual of the ℓ^∞-Selmer group of E/F tensored with $\mathbb{Q}_\ell$, viewed as a representation of $\mathrm{Gal}(F/\mathbb{Q})$.

2010 *Mathematics Subject Classification.* 11G40.

This result follows from Theorem 2.5 and Theorem 3.2(iii). The main question we would like to raise, of course, is whether this behaviour of L-functions or Selmer groups can be explained without appealing to the conjectures.

It is reasonably straightforward to construct such Galois extensions $F/\mathbb{Q}$. Consider for simplicity the case when C_{p^n} acts on C_q through C_p. Such fields $F = F_{p^n}$ are constructed as the compositum of a C_{p^n}-extension $K_{p^n}/\mathbb{Q}$ and an extension $F_p/\mathbb{Q}$ with Galois group $C_q \rtimes C_p$ that shares a common degree p subfield K_p with K_{p^n}. The irreducible faithful Artin representations of $\mathrm{Gal}(F/\mathbb{Q})$ are all of the form $\tau \otimes \chi$, for any irreducible p-dimensional representation of $\mathrm{Gal}(F_p/\mathbb{Q})$ and any 1-dimensional representation χ of $\mathrm{Gal}(K_{p^n}/\mathbb{Q})$ of order p^n (see Proposition 3.1).



For example, K_{p^n} could be the n^{th} layer of the p-cyclotomic tower of $\mathbb{Q}$, that is the unique degree p^n subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$, where $\zeta_{p^{n+1}}$ is a primitive p^{n+1}-th root of unity. This gives the following:

Corollary 1.2. *Suppose that $F_p/\mathbb{Q}$ is Galois with $\mathrm{Gal}(F_p/\mathbb{Q}) \cong C_q \rtimes C_p$ non-abelian, and that its degree p subfield K_p is the first layer of the p-cyclotomic extension of $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve and τ an irreducible faithful representation of $\mathrm{Gal}(F_p/\mathbb{Q})$. If Conjecture 2.1 holds, then for all finite order characters χ that factor through the p-cyclotomic extension with $\chi^{q-1} \neq \mathbf{1}$,*

$$\mathrm{ord}_{s=1} L(E, \tau \otimes \chi, s) \equiv 0 \mod p.$$

If τ is a representation of $\mathrm{Gal}(F/\mathbb{Q})$ such that $\tau = \mathrm{Ind}_{K/\mathbb{Q}} \psi$ for some subfield $K \subset F$, then we have an equality of L-functions $L(E, \tau, s) = L(E/K, \psi, s)$ for any elliptic curve $E/\mathbb{Q}$. In our setup, all irreducible faithful representations τ are induced from characters. More concretely, if $\mathrm{Gal}(F_{p^n}/\mathbb{Q}) \cong C_q \rtimes C_{p^n}$ is non-abelian, such that C_{p^n} acts on C_q through C_p, then $\tau = \mathrm{Ind}_{K_p/\mathbb{Q}} \psi$ where K_p is the degree p subfield of F_{p^n} and ψ is a primitive character of order qp^{n-1}. In particular, we get the following consequence for L-functions of certain modular forms.

Corollary 1.3. *Suppose that $F_p/\mathbb{Q}$ is Galois with $\mathrm{Gal}(F_p/\mathbb{Q}) \cong C_q \rtimes C_p$ non-abelian, and that its degree p subfield K_p is the first layer of the p-cyclotomic extension of $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve, let f_E be the modular form attached to E and let $\mathbf{f}_E$ be the Hilbert modular form which is the base-change of f_E to the (totally real cyclic) extension $K_p/\mathbb{Q}$. Assuming Conjecture 2.1, for any n such that $p^n \nmid q-1$ and primitive character ψ of $\mathrm{Gal}(F_pK_{p^n}/K_p) \cong C_{qp^{n-1}}$, we have*

$$\mathrm{ord}_{s=1} L(\mathbf{f}_E, \psi, s) \equiv 0 \mod p,$$

where K_{p^n} is the n^{th} layer of the p-cyclotomic extension of $\mathbb{Q}$.

Question 1.4. *Our approach relies on elliptic curves. Is the order of vanishing a multiple of p when the modular form doesn't correspond to an elliptic curve? (As the referee pointed out to us, one may be able to address weight 2 eigenforms by considering the group of rational points on the associated abelian variety.)*

Example 1.5. As a concrete example, take $p=3$ and $q=7$. For the degree 7 non-Galois extension F_1 (see diagram above) take the field $F_1 = \mathbb{Q}(\alpha)$ of discriminant $3^8 7^{12}$, where α is a root of $x^7 - 42x^5 - 70x^4 + 168x^3 + 126x^2 - 84x - 45$. As in the above discussion, take $K_{3^n} = \mathbb{Q}(\zeta_{3^{n+1}})^+$ and set $F_{3^n} = F_1 K_{3^n}$, the n^{th} layer

of the p-cyclotomic tower of F_1. The field F_3 is the Galois closure of F_1 and $\mathrm{Gal}(F_3/\mathbb{Q}) \cong C_7 \rtimes C_3$ non-abelian; this group is an analogue of a dihedral group with C_2 replaced by C_3.

The group $\mathrm{Gal}(F_3/\mathbb{Q}) \cong C_7 \rtimes C_3$ has three 1-dimensional representations that come from the C_3-quotient, and two 3-dimensional irreducible representations τ_0, τ_0', which are induced from 1-dimensional characters ψ_0, ψ_0' of C_7. The irreducible representations of $\mathrm{Gal}(F_{3^n}/\mathbb{Q}) \cong C_7 \rtimes C_{3^n}$ are the 1-dimensional representations lifted from the C_{3^n}-quotient, and 3-dimensional irreducibles that can all be written as $\tau = \tau_0 \otimes \chi$ or $\tau = \tau_0' \otimes \chi$ for some 1-dimensional χ; note that these can therefore also be expressed as $\tau = \mathrm{Ind}_{K_3/\mathbb{Q}} \psi$, where $\psi = \psi_0 \otimes \mathrm{Res}\, \chi$ or $\psi_0' \otimes \mathrm{Res}\, \chi$ is 1-dimensional. The faithful ones are precisely the ones with χ of maximal order, equivalently with ψ of order $7 \times 3^{n-1}$.

Now let $E/\mathbb{Q}$ be an elliptic curve. The L-function in Theorem 1.1 can be expressed in several ways: if, say, $\tau = \tau_0 \otimes \chi = \mathrm{Ind}_{K_3/\mathbb{Q}} \psi$ is 3-dimensional irreducible, then

$$L(E, \tau, s) = L(E, \tau_0 \otimes \chi, s) = L(E/K_3, \psi, s) = L(\mathbf{f}_E, \psi, s),$$

where $\mathbf{f}_E$ is as in Corollary 1.3.

In this setting, our prediction is that the order of vanishing of this L-function is necessarily a multiple of 3, so long as τ does not factor through $C_7 \rtimes C_3$ (equivalently if the order of χ is at least 9). As we will explain in §2–3, the corresponding statement is provably true for the Mordell–Weil group $E(F_{3^n})$, which is how we obtain the prediction for L-functions and Selmer groups.

Finally, let us note that it is possible to make a prediction for analytic ranks that do not involve twisted L-functions, although it becomes a little cumbersome. Using the subfield lattice of $F_{3^n}/\mathbb{Q}$ and inductivity of L-functions, one checks that

$$\frac{L(E/F_{3^n}, s) L(E/K_{3^{n-1}}, s)}{L(E/K_{3^n}, s) L(E/F_{3^{n-1}}, s)} = \prod_{\tau \text{ faithful}} L(E/\mathbb{Q}, \tau, s)^3,$$

Observe that the faithful representations $\tau : \mathrm{Gal}(F_{3^n}/\mathbb{Q}) \to \mathrm{GL}_3(\overline{\mathbb{Q}})$ have Galois conjugate images, since they are induced from Galois conjugate 1-dimensional ψ's. Thus, if we assume Conjecture 2.1 or Deligne's conjecture on Galois-equivariance of L-values [Del79, Conjecture 2.7ii], the orders of vanishing of their L-functions should all be equal, and hence the order of vanishing of the right-hand term in the above equation is a multiple of $3 \times 3 \times \frac{(7-1)(3^n - 3^{n-1})}{3^2} = 4 \times 3^n$. In particular, if the L-values at $s = 1$ are non-zero for $E/F_{3^{n-1}}$ and E/K_{3^n} (and hence for $E/K_{3^{n-1}}$), then the order of the zero of $L(E/F_{3^n}, s)$ must be a multiple of 4×3^n. More generally, the same technique yields the following result.

Corollary 1.6. *Let $F/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(F/\mathbb{Q}) \cong C_q \rtimes C_{p^n}$ non-abelian, where the image of C_{p^n} in $\mathrm{Aut}\, C_q$ has order p^r and $p^n \nmid q-1$. Suppose $E/\mathbb{Q}$ is an elliptic curve such that $L(E/K, 1) \neq 0$ for all proper subfields $K \subsetneq F$. If Conjecture 2.1 holds, then*

$$\mathrm{ord}_{s=1} L(E/F, s) \;\equiv\; 0 \mod p^{n-r}(p-1)(q-1).$$

Remark 1.7. At present we do not have examples where the orders of vanishing of such L-functions are non-zero, as their conductors appear to be too large for any extensive numerical search. We also cannot guarantee a zero at $s = 1$ by forcing the L-function to be essentially antisymmetric about that point: the twisting Artin representations τ (or $\tau \otimes \chi$) above are never self-dual, so the functional equation

relates $L(E,\tau)$ to $L(E,\tau^*)$ and the root number ("sign") cannot be used to force a zero. The latter is a general feature of our approach, see Remark 2.7.

Remark 1.8. As will be clear from §2–3, Theorem 1.1 applies generally to abelian varieties over number fields, rather than elliptic curves over $\mathbb{Q}$.

Remark 1.9. The Galois representation $H^1_{\text{ét}}(E,\mathbb{Q}_\ell)_{\mathbb{C}}\otimes\tau$ can be irreducible, so the multiplicity of the order of vanishing is not explained by a decomposition of the Galois representation. Moreover, the L-series is not the (formal) p^{th} power of another L-series. For example, if $G=C_7\rtimes C_9$ and v is a prime of good reduction of E such that Frobenius at v is an element of order 7 in G, then the Euler factor at v is $\frac{1}{(1-\zeta_7\alpha p^{-s})(1-\zeta_7\beta p^{-s})(1-\zeta_7^2\alpha p^{-s})(1-\zeta_7^2\beta p^{-s})(1-\zeta_7^4\alpha p^{-s})(1-\zeta_7^4\beta p^{-s})}$, which is visibly not a cube; here α and β are the Frobenius eigenvalues at v of E, and ζ_7 a suitable primitive 7-th root of unity.

Question 1.10. *For a self-dual Artin representation τ, the sign in the functional equation of $L(E,\tau,s)$ determines the parity of the order of vanishing at $s=1$. The normalised L-function $\Lambda(E,\tau,s)$ has the "clean" functional equation $\Lambda(E,\tau,s)=\pm\Lambda(E,\tau,2-s)$, so, in particular, the Taylor series expansion around $s=1$ has either only even terms or only odd terms. Is there any such effect for the L-functions in Theorem 1.1, i.e. can one normalise them so that the only non-zero coefficients in the Taylor expansion $\Lambda(E,\tau,s)=\sum a_k(s-1)^k$ are the a_k with $p|k$?*

2. Birch–Swinnerton-Dyer conjecture and the Schur index

Statements that concern the Birch–Swinnerton-Dyer conjecture usually suppose properties about a given L-function so as to ascertain information about the rank (e.g. Coates–Wiles, Gross–Zagier, Kolyvagin). Our approach is somewhat peculiar: we are traversing the opposite direction by using the Mordell–Weil group to derive a feature of the L-function. We rely on the following generalisation of the Birch–Swinnerton-Dyer conjecture.

Conjecture 2.1 (Birch–Swinnerton-Dyer, Deligne–Gross; see [Roh90] p.127)**.** *Let A be an abelian variety over a number field K, and let τ be a representation of* $\mathrm{Gal}(F/K)$ *for some finite Galois extension F/K. Then $L(A/K,\tau,s)$ has analytic continuation to $\mathbb{C}$ and*

$$\operatorname{ord}_{s=1} L(A/K,\tau,s)=\langle A(F)_{\mathbb{C}},\tau\rangle,$$

where $A(F)_{\mathbb{C}}$ is the natural representation of $\mathrm{Gal}(F/K)$ *on $A(F)\otimes_{\mathbb{Z}}\mathbb{C}$.*

The key observation is that since the Galois group acts on a $\mathbb{Z}$-lattice, $A(F)_{\mathbb{C}}$ is a rational representation. Therefore certain complex irreducible representations τ cannot appear with multiplicity 1 in $A(F)_{\mathbb{C}}$; this aspect is measured by the Schur index $m_{\mathbb{Q}}(\tau)$. In contrast, the analogous property is not obvious (and unknown in general) for either the L-function of an abelian variety or the $\mathbb{Q}_\ell$-representation on the dual Selmer group $X_\ell(A/F)$.

Definition 2.2. Let G be a finite group and $\mathcal{F}$ a subfield of $\mathbb{C}$. We say a complex representation τ of G is realisable over $\mathcal{F}$ if it is conjugate to a representation that factors as $G\to\mathrm{GL}_n(\mathcal{F})\subset\mathrm{GL}_n(\mathbb{C})$ for some n. The Schur index $m_{\mathcal{F}}(\tau)$ is the maximal integer m such that for all representations σ of G that are realisable over $\mathcal{F}$, the multiplicity $\langle\tau,\sigma\rangle$ is a multiple of m.

Example 2.3. The Schur index $m_{\mathbb{Q}}(\tau)$ of the 2-dimensional irreducible representation τ of the quaternion group Q_8 is 2. Hence τ, despite having rational trace, cannot be realised by matrices in $\mathrm{GL}_2(\mathbb{Q})$; however $\tau \oplus \tau$ is realisable in $\mathrm{GL}_4(\mathbb{Q})$.

Remark 2.4. Note that for any field $\mathcal{F}$, $m_{\mathcal{F}}(\tau) \leq \dim \tau$ as the regular representation is realisable over $\mathbb{Q}$. In fact $m_{\mathcal{F}}(\tau)$ always divides the dimension $\dim \tau$, see e.g. [Isa76, Corollary 10.2].

Theorem 2.5. *Let F/K be a Galois extension of number fields, and let τ be an irreducible Artin representation of* $\mathrm{Gal}(F/K)$. *Then for all abelian varieties A/K, the multiplicity of τ in $A(F)_{\mathbb{C}}$ is divisible by $m_{\mathbb{Q}}(\tau)$. In addition:*

(i) If Conjecture 2.1 holds, then $\mathrm{ord}_{s=1} L(A/K, \tau, s)$ *is divisible by $m_{\mathbb{Q}}(\tau)$;*
(ii) If $Ш(A/F)[\ell^\infty]$ is finite for some prime ℓ, then $\langle X_\ell(A/F), \tau\rangle$ is divisible by $m_{\mathbb{Q}}(\tau)$.

Proof. By construction, $A(F)_{\mathbb{C}}$ is realisable over $\mathbb{Q}$ so by definition $m_{\mathbb{Q}}(\tau)$ divides $\langle A(F)_{\mathbb{C}}, \tau\rangle$. The L-function statement now follows directly from Conjecture 2.1. If $Ш(A/F)[\ell^\infty]$ is finite, then $X_\ell(A/F) \cong A(F) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ as $\mathbb{Q}_\ell[\mathrm{Gal}(F/K)]$-modules, from which the second part follows. □

Remark 2.6. Without the finiteness assumption on Ш, the dual Selmer group $X_\ell(A/F)$ is not known to be a rational or even an orthogonal representation of the Galois group (although it is known to be self-dual, see [DD09]). Thus, as the ℓ-adic Schur index $m_{\mathbb{Q}_\ell}(\tau)$ can be 1, there is no obvious representation-theoretic reason for the multiplicity of τ in $X_\ell(A/F)$ to be a multiple of $m_{\mathbb{Q}}(\tau)$; see Theorem 3.2 for an example of such a τ.

Remark 2.7. The reason for the restriction on the order of vanishing of the L-function is fairly well-understood for self-dual representations τ with Schur index 2 (for example the quaternion representation in Example 2.3). In this case the conjectural functional equation is of the form $L(A, \tau, s) = \pm L(A, \tau, 2-s) \times$ (Γ-factors and exponential). So the parity of the order of vanishing at $s = 1$ is determined by the sign $\pm$, which is given by the global root number $W(A, \tau)$ and known to be $+$ whenever τ is symplectic and in many cases when τ is orthogonal with Schur index 2, see [Roh96, Proposition 2] and [Sab07, Theorem 0.1].

It is tempting to use the sign in the functional equation to force a zero of the L-function for a representation τ with large Schur index $m = m_{\mathbb{Q}}(\tau)$. If Conjecture 2.1 is true, the order of vanishing is a fortiori at least m. Curiously enough, this is impossible to achieve: if $m > 2$, the representation τ cannot be self-dual by the Brauer–Speiser theorem. Thus the functional equation relates $L(A, \tau, s)$ to $L(A, \tau^*, 2-s)$, and the root number cannot be used to force the L-function to vanish at $s = 1$.

3. Schur indices in $C_q \rtimes C_{p^n}$

We now compute the Schur indices of representations of $C_q \rtimes C_{p^n}$ appearing in Theorem 1.1. We only prove that the Schur index is divisible by p without determining it exactly, so the bounds on orders of vanishing of L-functions that we have given may be suboptimal. For example, if τ is an irreducible faithful representation of $C_{19} \rtimes C_{3^4}$ (with the largest possible action), then $m_{\mathbb{Q}}(\tau) = 9$.

For a field $\mathcal{F}$ and representation τ, we let $\mathcal{F}(\tau)$ denote the finite abelian extension of $\mathcal{F}$ generated by the values of the trace of τ. We further let ζ_m denote a primitive m^{th} root of unity and $N_{\mathcal{F}/\mathcal{K}}$ be the norm map for any field extension $\mathcal{F}/\mathcal{K}$.

Proposition 3.1. *Let p,q be distinct odd primes and $G = C_q \rtimes C_{p^n}$, where the image of C_{p^n} in $\operatorname{Aut} C_q$ has order p^r. Let τ be a complex irreducible representation of G. Write $X = C_q \times C_{p^{n-r}} \lhd G$.*
(i) If τ is unfaithful then τ is lifted either from C_{p^n} or from $C_q \rtimes C_{p^{n-1}}$.
(ii) If τ is faithful, then $\dim\tau = p^r$ and there is a faithful 1-dimensional representation of X such that $\tau = \operatorname{Ind}_X^G \psi$. Conversely, the induction of a faithful 1-dimensional representation ψ of X gives a faithful irreducible representation of G.
(iii) Every faithful irreducible representation τ of G may be written as $\tau_r \otimes \chi$ for some faithful irreducible representation τ_r of $C_q \rtimes C_{p^r}$ and faithful 1-dimensional representation χ of C_{p^n}.
(iv) If $\tau = \operatorname{Ind}_X^G \psi$ is faithful and $\mathcal{F} \subset \mathbb{C}$ is a field, then $\mathcal{F}(\psi) = \mathcal{F}(\zeta_{p^{n-r}}, \zeta_q)$ and $\mathcal{F}(\tau) = \mathcal{F}(\zeta_{p^{n-r}}, \sum_{t\in H} \zeta_q^t)$, where $H \le (\mathbb{Z}/q\mathbb{Z})^\times$ is the subgroup of order p^r.
(v) If $\tau = \operatorname{Ind}_X^G \psi$ is faithful and $\mathcal{F} \subset \mathbb{C}$ is a field such that $[\mathcal{F}(\psi):\mathcal{F}(\tau)] = p^r$, then the Schur index $m_{\mathcal{F}}(\tau) = 1$ if and only if $\zeta_{p^{n-r}}$ is in the image of $N_{\mathcal{F}(\psi)/\mathcal{F}(\tau)}$.

Proof. The group G has presentation $G = \langle a, b \mid a^q = b^{p^n} = \mathrm{id}, bab^{-1} = a^j\rangle$ where j has order p^r modulo q. The subgroup X is $\langle a, b^{p^r}\rangle$; it is the centraliser of C_q. For a representation ψ of X and a element $g \in G$ we write ${}^g\psi$ for the conjugate representation defined by ${}^g\psi(h) = \psi(ghg^{-1})$.

(i) The maximal quotients of G are C_{p^n} and (if $r < n$) $C_q \rtimes C_{p^{n-1}}$, so if τ is not faithful, it factors through one of these.

(ii) By [Ser77, Proposition 25], every faithful representation of G is necessarily induced from a 1-dimensional representation ψ of X; in particular $\dim\tau = p^r$. Moreover, since $\ker\psi$ is normal in G (as X is normal in G and $\ker\psi$ is characteristic in the cyclic group X), we have $\ker\psi \subseteq \ker\tau$, and hence ψ must be faithful.

Conversely, $h \mapsto b^k h b^{-k}$ are distinct automorphisms of X for $0 \le k < p^r - 1$, so if ψ is a faithful 1-dimensional representation of X, then $\psi, {}^b\psi, \dots, {}^{b^{p^r-1}}\psi$ are all distinct. Thus $\langle\tau,\tau\rangle = \langle\psi, \operatorname{Res}_X^G \operatorname{Ind}_X^G \psi\rangle = \langle\psi, \bigoplus_{0\le k<p^r} {}^{b^k}\psi\rangle = 1$ by Frobenius reciprocity and Mackey's formula, and so τ is irreducible. It is clearly faithful by (i).

(iii) Let $\tau = \operatorname{Ind}_X^G \psi$, for some faithful 1-dimensional ψ of order qp^{n-r}. We can rewrite this as $\psi = \psi_q \otimes \psi_{p^{n-r}}$ where ψ_m has order m. Now $\tau_r = \operatorname{Ind}_X^G \psi_q$ is the inflation of a faithful representation of $C_q \rtimes C_{p^r}$. Let χ be a 1-dimensional representation of G which factors through C_{p^n} such that $\operatorname{Res}_X^G \chi = \psi_{p^{n-r}}$. The push-pull formula shows that $\tau = \tau_r \otimes \chi$, as claimed.

(iv) If τ is faithful, then by (ii) ψ is a faithful 1-dimensional representation of $X \cong C_{qp^{n-r}}$, hence $\mathcal{F}(\psi) = \mathcal{F}(\zeta_{qp^{n-r}})$. To compute $\mathcal{F}(\tau)$, it suffices to compute the induced character on the conjugacy classes of G which have nonempty intersection with X. Since $X \lhd G$, it follows that $\mathcal{F}(\tau) = \mathcal{F}(\operatorname{Res}_X^G \tau)$.

Note that b^{p^r} is central in G and τ is irreducible so $\tau(b^{p^r})$ must be scalar by Schur's lemma; as $\operatorname{Res}_X^G \tau$ contains ψ as a constituent, this scalar is multiplication-by-$\zeta_{p^{n-r}}$, hence $\zeta_{p^{n-r}} \in \mathcal{F}(\tau)$. For $a^x b^{p^r y} \in X$ we have $\operatorname{tr}\tau(a^x b^{p^r y}) = \zeta_{p^{n-r}}^y \operatorname{tr}\tau(a^x)$, so $\mathcal{F}(\tau)$ is generated over $\mathcal{F}$ by $\zeta_{p^{n-r}}$ and the traces $\operatorname{tr}\tau(a^x)$) for $1 \le x \le q$.

As in the proof in (ii), $\operatorname{Res}_X^G \tau = \bigoplus_{0\le k<p^r} {}^{b^k}\psi$, so $\operatorname{tr}\tau(a^x) = \sum_{t\in H} \zeta_q^{xt}$, where H is the unique index subgroup of order p^r contained in $(\mathbb{Z}/q\mathbb{Z})^\times$. Note that for any

polynomial $f \in \mathbb{Q}[X]$, $f(\zeta_q)$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate to $f(\zeta_q^x)$ whenever $q \nmid x$, and hence $f(\zeta_q^x) \in \mathbb{Q}(f(\zeta_q))$ since $\mathbb{Q}(f(\zeta_q))/\mathbb{Q}$ is abelian. In particular, letting $f(X) = \sum_{t\in H} X^t$ (where we fix representatives for H), we see that $\sum_{t\in H} \zeta_q^{xt} \in \mathbb{Q}(\sum_{t\in H} \zeta_q^t)$ for all x. Hence $\mathcal{F}(\tau) = \mathcal{F}(\zeta_{p^{n-r}}, \sum_{t\in H} \zeta_q^t)$ as claimed.

(v) First note that X is normal, abelian and equal to its own centraliser, $X = C_G(X)$, as otherwise $b^k \in C_G(X)$ for some k with $p^r \nmid k$ which doesn't commute with a. Since by assumption the (abelian) extension $\mathcal{F}(\psi)/\mathcal{F}(\tau)$ has degree p^r, the representation ψ must have p^r distinct $\mathrm{Gal}(\mathcal{F}(\psi)/\mathcal{F}(\tau))$-conjugates, which then must be precisely the constituents of $\mathrm{Res}^G_X \tau$. Thus (G, X, τ) is an $\mathcal{F}$-triple, in the terminology of [Isa76, Definition 10.5]. Noting that $G = XC_{p^n}$, it then follows from [Isa76, Theorem 10.10] that $m_{\mathcal{F}}(\tau) = 1$ if and only if $\zeta_{p^{n-r}} \in N_{\mathcal{F}(\psi)/\mathcal{F}(\tau)}\mathcal{F}(\psi)$. □

Theorem 3.2. *Let p, q be distinct odd primes and $G = C_q \rtimes C_{p^n}$, where the image of C_{p^n} in $\mathrm{Aut}\, C_q$ has order p^r and $0 < r \leq n$. Let τ be a complex irreducible faithful representation of G. Then:*
(i) The Schur index $m_{\mathbb{Q}}(\tau) = p^s$ for some $0 < s \leq r$ if $p^n \nmid q-1$, and is 1 otherwise;
(ii) The Schur index $m_{\mathbb{Q}_q}(\tau) = m_{\mathbb{Q}}(\tau)$;
(iii) The Schur index $m_{\mathbb{Q}_\ell}(\tau) = 1$ for every prime $\ell \neq q$.

Proof. (iii) It is a general fact that if $\ell \nmid |G|$, then $m_{\mathbb{Q}_\ell}(\tau) = 1$; see for example [Gow75]. The Corollary in [Gow75] states more generally that if τ is irreducible modulo ℓ, then $m_{\mathbb{Q}_\ell}(\tau) = 1$; this will be our approach for the case $\ell = p$. To see that this holds, let σ be an irreducible constituent of τ modulo p. Now the eigenvalues of $\tau(a)$ (using the notation from the first paragraph of the proof of Proposition 3.1) are primitive q^{th} roots of unity, hence this also holds for σ. Let v be an eigenvector for $\sigma(a)$ with eigenvalue ζ. Then $\sigma(b^{-1})v$ is also an eigenvector for $\sigma(a)$ with eigenvalue ζ^j. As j has order p^r modulo q (note $q \neq p$), σ has p^r distinct eigenvalues, so $\dim \sigma = \dim \tau$ and hence τ is irreducible modulo p.

(ii) The global Schur index $m_{\mathbb{Q}}(\tau)$ is well known to equal the lowest common multiple of the local Schur indices $m_{\mathbb{Q}_v}(\tau)$ for all places v of $\mathbb{Q}$ (see for example [Olt09, Theorem 2.4]). Now τ is not self-dual (as G has odd order) so $m_{\mathbb{R}}(\tau) = 1$ hence the result is immediate from (iii).

(i) We prove instead the same statement for $m_{\mathbb{Q}_q}(\tau)$; the global statement for $m_{\mathbb{Q}}(\tau)$ then follows from (ii). Write $\tau = \mathrm{Ind}^G_X \psi$, as in Proposition 3.1(ii). By Proposition 3.1(iv), the extension $\mathbb{Q}_q(\psi)/\mathbb{Q}_q(\tau)$ is totally ramified of degree p^r, and so by (v) it suffices to check whether $\zeta_{p^{n-r}}$ is in the image of the norm map $N_{\mathbb{Q}_q(\psi)/\mathbb{Q}_q(\tau)}$.

By local class field theory, the subgroup of $\mathcal{O}^\times_{\mathbb{Q}_q(\tau)}$ consisting of norms from $\mathcal{O}^\times_{\mathbb{Q}_q(\psi)}$ has index p^r. Furthermore, as the extension is tame, $u \in \mathcal{O}^\times_{\mathbb{Q}_q(\tau)}$ is a norm if and only if its image $\bar{u}$ in the residue field $\mathbb{F}_{\mathbb{Q}_q(\tau)}$ of $\mathbb{Q}_q(\tau)$ is a norm from the residue field of $\mathbb{Q}_q(\psi)$; as the two residue fields are the same, this is equivalent to $\bar{u}$ being of the form $\bar{u} = x^{p^l}$ for some $x \in \mathbb{F}_{\mathbb{Q}_q(\tau)}$.

Thus we are reduced to checking whether $\mathbb{F}_{\mathbb{Q}_q(\tau)}$ contains a primitive p^n-th root of unity. Since $\mathbb{Q}_q(\tau)/\mathbb{Q}_q(\zeta_{p^{n-r}})$ is totally ramified (Proposition 3.1(iv)), by Hensel's Lemma this happens if and only if $\zeta_{p^n} \in \mathbb{Q}_q(\zeta_{p^{n-r}})$.

If $p^n | q-1$, then $\zeta_{p^n} \in \mathbb{Q}_q \subseteq \mathbb{Q}_q(\zeta_{p^{n-r}})$, and hence $m_{\mathbb{Q}_q}(\tau) = 1$.

Conversely, if $p^n \nmid q-1$, then $q \bmod p^n$ is a non-trivial element of p-power order (since $r > 0$ implies $q \equiv 1 \bmod p$) in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. In particular, $\mathrm{Gal}(\mathbb{Q}_q(\zeta_{p^n})/\mathbb{Q}_q)$

contains an element of order p. All such elements fix $\zeta_{p^{n-r}}$, and consequently $\mathbb{Q}_q(\zeta_{p^{n-r}}) \neq \mathbb{Q}_q(\zeta_{p^n})$. It follows that $\zeta_{p^n} \notin \mathbb{Q}_q(\zeta_{p^{n-r}})$ and so $m_{\mathbb{Q}_q}(\tau) \neq 1$. It now follows from Remark 2.4 and Proposition 3.1(ii) that the Schur index is $m_{\mathbb{Q}_q}(\tau) = p^s$ for some $0 < s \leq r$. □

Acknowledgements. The authors would like to thank Tim Dokchitser for the useful discussions that led to this paper and the anonymous referee for their comments. The second author is supported by a Royal Society University Research Fellowship.

References

[DD09] T. Dokchitser and V. Dokchitser. Self-duality of Selmer groups. *Math. Proc. Cambridge Philos. Soc.*, 146:257–267, 2009.

[Del79] P. Deligne. Valeurs de fonctions L et périodes d'intégrales. In *Automorphic Forms, Representations and L-Functions, Proc. Symp. Pure Math Vol 33 - Part 2*, pages 313–346. Amer. Math. Soc., 1979.

[Gow75] R. Gow. Schur indices and modular representations. *Math. Z.*, 144(2):97–99, 1975.

[Isa76] I. Isaacs. *Character theory of finite groups*. Academic Press Inc., 1976.

[Olt09] G. Olteanu. Computation and applications of Schur indices. In *Proceedings of the International Conference on Modules and Representation Theory*, pages 149–157. Cluj University Press, 2009.

[Roh90] D. Rohrlich. The vanishing of certain Rankin-Selberg convolutions. In *Automorphic Forms and Analytic Number Theory*, pages 123–133. Univ. Montréal, Montréal, QC, 1990.

[Roh96] D. Rohrlich. Galois theory, elliptic curves, and root numbers. *Compositio Mathematica*, 100(3):311–349, 1996.

[Sab07] M. Sabitova. Root numbers of abelian varieties. *Trans. Amer. Math. Soc.*, 359:4259–4284, 2007.

[Ser77] J. Serre. *Linear representations of finite groups*. Springer Science & Business Media, 1977.

Faculty of Natural and Mathematical Sciences, Strand Campus, King's College London, London, WC2R 2LS, United Kingdom

E-mail address: matthew.bisatt@kcl.ac.uk

E-mail address: vladimir.dokchitser@kcl.ac.uk